UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,102	12/02/2003	Masato Yamamichi	2003_1742A	5711

52349 7590 04/02/2008

WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
04/02/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/725,102	YAMAMICHI ET AL.	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47,49 and 50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47, 49, & 50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the Request for Continued Examination filing of 12/17/2007. In light of the applicant's amendments, the examiner hereby withdraws his previous Specification Objection and Claim 26 Objection. In light of the applicant's claims amendments and remarks, the examiner hereby withdraws his Statutory Double Patenting rejection. The examiner acknowledges the cancellation of Claims 48 & 51. Claims 1-47, 49, & 50 are pending and have been considered as follows.

Claim Objections

1. Claims 1-3, 9, 11, 23-25, 41, & 45 are objected to because of the following informalities:
   - Claim 1 lines 5, 6, 8, 10, 12, 15, 17, 19, 21, 24, & 27 recite the term "operable" which should be "…configured…";
   - Claim 2 lines 3, 4, 9, & 11 recite the term "operable" which should be "…configured…";
   - Claim 3 lines 4, 5, 7, 9, & 11 recite the term "operable" which should be "…configured…";
   - Claim 9 lines 3 & 4 recite the term "operable" which should be "…configured…";
   - Claim 11 lines 3 & 4 recite the term "operable" which should be "…configured…";
   - Claim 23 lines 2 & 3 recite the term "operable" which should be "…configured…";
   - Claim 24 lines 8, 10, 12, 14, 17, & 20 recite the term "operable" which should be "…configured…";

- Claim 25 lines 6 & 8 recite the term "operable" which should be "…configured…";
- Claim 41 lines 7, 8, & 11 recite the term "operable" which should be "…configured…";
- Claim 45 lines 6 & 8 recite the term "operable" which should be "…configured…";

Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3, 4, 24, 46, 47, 49, & 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro et al. (US-5937066-A) in view of Gennaro et al. (US-5907618-A).

Claim 1:

Gennaro et al. (US-5937066-A) disclose a key agreement system comprising a shared-key generation apparatus and a shared-key recovery apparatus, each apparatus establishing therein a same shared key in secrecy comprising,

- "a seed-value generating unit operable to generate a seed value" (i.e. "Alice and Bob exchange a random S (step 902)") [column 17 line 27];
- "a first shared-key generating unit operable to generate a verification value and a shared key, from the seed value" (i.e. "Alice derives from S a value KG for each agent, by hashing S and the respective agent's ID (step 904)") [column 17 lines 29-30];

- "a first encryption unit operable to encrypt the verification value to generate first encryption information" (i.e. "Alice encrypts the KG values under the respective agents' public keys (step 906)… PUa1: public key for Alice's first agent…KGa1: key-generating key for Alice's first agent") [column 17 lines 31,32, 40, & 45];
- "a second encryption unit operable to encrypt the seed value based on the verification value, to generate second encryption information" (i.e. "Alice encrypts the KG values under the respective agents' public keys (step 906)…PUa2: public key for Alice's second agent… KGa2: key-generating key for Alice's second agent") [column 17 lines 31,32, 41, & 46];
- "a transmitting unit operable to transmit the first encryption information and the second encryption information" (i.e. "Alice sends to Bob the SKR phase 1 data block B1 (FIG. 11) composed of: T1, ePUa1(KGa1), ePUa2(KGa2), ePUb1(KGb1), and ePUb2(KGb2) (step 908)") [column 17 lines 33-35];
- "wherein the shared-key recovery apparatus include: a receiving unit operable to receive the first encryption information and the second encryption information" (i.e. "Optional Transmission of S or K: If needed, SKR can transmit either or both S and K") [column 19 lines 3-4];
- "wherein the shared-key recovery apparatus include: a second shared-key generating unit operable to generate a second decryption verification value and a decryption shared key, from the decryption seed value and according to a same method as used in the first shared-key generating unit" (i.e. "Alice derives from S a value KG for each agent, by hashing S and the respective agent's ID (step 904)") [column 17 lines 29-30];

- "wherein the first encryption information and the second encryption information are separate pieces of information" (i.e. "PUa1: public key for Alice's first agent… PUa2: public key for Alice's second agent") [column 17 lines 40-41];

but, they do not explicitly disclose,

- "wherein the shared-key recovery apparatus include: a first decryption unit operable to decrypt the first encryption information, to generate a first decryption verification value," although Gennaro et al. (US-5907618-A) do suggest a hash, as recited below;
- "wherein the shared-key recovery apparatus include: a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value, to generate a decryption seed value," although Gennaro et al. (US-5907618-A) do suggest a hash, as recited below;
- "wherein the shared-key recovery apparatus include: a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted," although Gennaro et al. (US-5907618-A) do suggest verification based on at least one hash, as recited below;
- "wherein the shared-key recovery apparatus include: an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key," although Gennaro et al. (US-5907618-A) do suggest verification, as recited below;
- "wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses," although Gennaro et al. (US-5907618-A) do suggest a sender and receiver, as recited below;

however, Gennaro et al. (US-5907618-A) do disclose,

- "The hash value form a check on the decryption" [column 13 lines 31];
- "from Alice (step 1002), Bob locates the previously cached values KGa1-KGb2, using the hash value Hash(B1) in the block B2 as an index (step 1004)" [column 14 lines 3-5];
- "if there are multiple sets of key recovery agents as in the present example, then Bob must ensure that all of the various versions of K agree if he is to fully validate the recovery information" [column 14 lines 25-28];
- "As disclosed in the copending Gennaro et al. application, the decryption procedure 1200 may be keyed to the receiver verification steps so that the message is not decrypted unless all or a specified subset of the key recovery fields in data block B1 and B2 have been verified" [column 14 lines 51-56];
- "Bob…Alice" [column 11 lines 42 & 45];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the shared-key recovery apparatus include: a first decryption unit operable to decrypt the first encryption information, to generate a first decryption verification value" and "wherein the shared-key recovery apparatus include: a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value, to generate a decryption seed value" and "wherein the shared-key recovery apparatus include: a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted" and "wherein the shared-key recovery apparatus include: an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key" and

"wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses," in the invention as disclosed by Gennaro et al. (US-5937066-A) since it is reasonable to expect that Gennaro et al. would combine elements from both of his own inventions for the purposes of decryption and verification.

Claims 3, 46, & 47:

Gennaro et al. (US-5937066-A) disclose a shared-key generation apparatus that notifies a shared-key recovery apparatus about a shared key in secrecy, a shared-key generating method used in a shared-key generation apparatus that notifies a shared-key recovery apparatus about a shared key, in secrecy, the shared-key generating method, and a shared-key generating program embodied on a computer-readable storage medium and used in a shared-key generation apparatus that notifies a shared-key recovery apparatus about a shared key, in secrecy, the shared-key generating program causing the shared-key generation apparatus to perform a method comprising,

- "a seed-value generating unit operable to generate a seed value" (i.e. "Alice and Bob exchange a random S (step 902)") [column 17 line 27];
- "a shared-key generating unit operable to generate a verification value and a shared key, from the seed value" (i.e. "Alice derives from S a value KG for each agent, by hashing S and the respective agent's ID (step 904)") [column 17 lines 29-30];
- "a first encryption unit operable to encrypt the verification value to generate first encryption information" (i.e. "Alice encrypts the KG values under the respective agents' public keys (step 906)… PUa1: public key for Alice's first agent…KGa1: key-generating key for Alice's first agent") [column 17 lines 31,32, 40, & 45];

- "a second encryption unit operable to encrypt the seed value based on the verification value, to generate second encryption information" (i.e. "Alice encrypts the KG values under the respective agents' public keys (step 906)…PUa2: public key for Alice's second agent… KGa2: key-generating key for Alice's second agent") [column 17 lines 31,32, 41, & 46];
- "a transmitting unit operable to transmit the first encryption information and the second encryption information" (i.e. "Alice sends to Bob the SKR phase 1 data block B1 (FIG. 11) composed of: T1, ePUa1(KGa1), ePUa2(KGa2), ePUb1(KGb1), and ePUb2(KGb2) (step 908)") [column 17 lines 33-35];
- "wherein the first encryption information and the second encryption information are separate pieces of information" (i.e. "PUa1: public key for Alice's first agent… PUa2: public key for Alice's second agent") [column 17 lines 40-41];

but, they do not explicitly disclose,

- "wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses," although Gennaro et al. (US-5907618-A) do suggest a sender and receiver, as recited below;

however, Gennaro et al. (US-5907618-A) do disclose,

- "Bob…Alice" [column 11 lines 42 & 45];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses," in the invention as disclosed by Gennaro et al. (US-5937066-A) since it is reasonable to expect that Gennaro et al. would combine elements from both of his own inventions for the purposes of decryption and verification.

Claim 4:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key generation apparatus that notifies a shared-key recovery apparatus about a shared key in secrecy, as in Claim 3 above, further comprising,

- "the seed-value generating unit generates a random number, as the seed value" (i.e. "Alice and Bob exchange a random S (step 902)") [column 17 line 27].

Claims 24, 49, & 50:

Gennaro et al. (US-5937066-A) disclose a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a verification value and a shared key from the seed value, encrypting the verification value to generate first encryption information, encrypting the seed value based on the verification value to generate second encryption information, and transmitting the first encryption information and the second encryption information, the shared-key recovery apparatus, a shared-key recovery method used in a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a verification value and a shared key from the seed value, encrypting the verification value to generate first encryption information, encrypting the

seed value based on the verification value to generate second encryption information, and transmitting the first encryption information and the second encryption information, the shared-key recovery method, and a shared-key recovery program embodied on a computer readable storage medium and used in a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a verification value and a shared key from the seed value, encrypting the verification value to generate first encryption information, encrypting the seed value based on the verification value to generate second encryption information, and transmitting the first encryption information and the second encryption information, the shared key recovery program causing the shared-key recovery apparatus to perform a method comprising,

- "a receiving unit operable to receive the first encryption information and the second encryption information" (i.e. "Optional Transmission of S or K: If needed, SKR can transmit either or both S and K") [column 19 lines 3-4];
- "a shared-key generating unit operable to generate a second decryption verification value and a decryption shared key, from the decryption seed value and according to a same method as used in the shared-key generation apparatus" (i.e. "Alice derives from S a value KG for each agent, by hashing S and the respective agent's ID (step 904)") [column 17 lines 29-30];
- "wherein the first encryption information and the second encryption information are separate pieces of information" (i.e. "PUa1: public key for Alice's first agent… PUa2: public key for Alice's second agent") [column 17 lines 40-41];

but, they do not explicitly disclose,

- "a first decryption unit operable to decrypt the first encryption information, to generate a first decryption verification value," although Gennaro et al. (US-5907618-A) do suggest a hash, as recited below;
- "a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value, to generate a decryption seed value," although Gennaro et al. (US-5907618-A) do suggest a hash, as recited below;
- "a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted," although Gennaro et al. (US-5907618-A) do suggest verification based on at least one hash, as recited below;
- "an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key," although Gennaro et al. (US-5907618-A) do suggest verification, as recited below;
- "wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses," although Gennaro et al. (US-5907618-A) do suggest a sender and a receiver, as recited below;

however, Gennaro et al. (US-5907618-A) do disclose,

- "The hash value form a check on the decryption" [column 13 lines 31];
- "from Alice (step 1002), Bob locates the previously cached values KGa1-KGb2, using the hash value Hash(B1) in the block B2 as an index (step 1004)" [column 14 lines 3-5];

- "if there are multiple sets of key recovery agents as in the present example, then Bob must ensure that all of the various versions of K agree if he is to fully validate the recovery information" [column 14 lines 25-28];
- "As disclosed in the copending Gennaro et al. application, the decryption procedure 1200 may be keyed to the receiver verification steps so that the message is not decrypted unless all or a specified subset of the key recovery fields in data block B1 and B2 have been verified" [column 14 lines 51-56];
- "Bob…Alice" [column 11 lines 42 & 45];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a first decryption unit operable to decrypt the first encryption information, to generate a first decryption verification value" and "a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value, to generate a decryption seed value" and "a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted" and "an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key" and "wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses," in the invention as disclosed by Gennaro et al. (US-5937066-A) since it is reasonable to expect that Gennaro et al. would combine elements from both of his own inventions for the purposes of decryption and verification.

4. Claims 2, 5-23, & 25-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro et al. (US-5937066-A) in view of Gennaro et al. (US-5907618-A) and in further view of Hoffstein et al. (WO-9808323-A1).

Claim 2:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a key agreement system comprising a shared-key generation apparatus and a shared-key recovery apparatus, each apparatus establishing therein a same shared key in secrecy, as in Claim 1 above, but their combination do not disclose,

- "an obtaining unit operable to obtain a content," although Hoffstein et al. do suggest reception of information, as recited below;
- "an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content," although Hoffstein et al. do suggest public key encryption, as recited below;
- "the transmitting unit further transmits the encrypted content," although Hoffstein et al. do suggest communicating encrypted data/information, as recited below;
- "the receiving unit further receives the encrypted content," although Hoffstein et al. do suggest receiving encrypted data/information, as recited below;
- "a decryption unit operable to decrypt the received encrypted content using the decryption shared key, to generate a decrypted content," although Hoffstein et al. do suggest decryption of data/information, as recited below;
- "an outputting unit operable to output the decrypted content," although Hoffstein et al. do suggest decrypting and outputting data/information, as recited below;

however, Hoffstein et al. do disclose,

- [Fig 4 Box# 420 illustrates obtaining data/information];
- "The encoding technique of an embodiment of the public key cryptosystem hereof uses a mixing system based on polynomial algebra and reduction modulo two numbers, p and q, while the decoding technique uses an unmixing system whose validity depends on the elementary probability theory" [page 9];
- "Communication is via transceiver…" [page 8 lines 22-24];
- [Fig 5 Box# 530 illustrates receiving encrypted data/information];
- "The decoding for this matrix example is described next…" [page 20];
- "Finally Dan computes…to recover the original message m" [page 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "an obtaining unit operable to obtain a content" and "an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content" and "the transmitting unit further transmits the encrypted content" and "the receiving unit further receives the encrypted content" and "a decryption unit operable to decrypt the received encrypted content using the decryption shared key, to generate a decrypted content" and "an outputting unit operable to output the decrypted content," in the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 5-7:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key generation apparatus that notifies a shared-key recovery apparatus about a shared key in secrecy, as in Claim 3 above, but their combination do not disclose,

- "the shared-key generating unit performs a one-way function on the seed value to generate a functional value, and generates the verification value and the shared key from the functional value," although Hoffstein et al. do suggest the usage of polynomials in a public key encryption scheme, as recited below;
- "the shared-key generating unit performs, on the seed value, a hash function as the oneway function, to generate the functional value," although Hoffstein et al. do suggest the usage of polynomials in a public key encryption scheme, as recited below;
- "the shared-key generating unit generates the verification value by setting a part of the functional value as the verification value, and generates the shared key by setting another part of the functional value as the shared key," although Hoffstein et al. do suggest the usage of polynomials in a public key encryption/decryption scheme, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];
- "In order to decode the message e, Dan first uses his private key f to compute the polynomial" [page 17];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the shared-key generating unit performs a one-way function on the seed value to generate a functional value, and generates the verification value and the shared key from the functional value" and "the shared-key generating unit performs, on the seed value, a hash function as the oneway function, to generate the functional value" and "the shared-key generating unit generates the verification value by setting a part of the functional value as the verification value, and generates the shared key by setting another part of the functional value as the shared key," in the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 8-10:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key generation apparatus that notifies a shared-key recovery apparatus about a shared key in secrecy, as in Claim 3 above, but their combination do not disclose,

- "the shared-key generating unit performs a one-way function on the seed value to generate a functional value, and generates the verification value, the shared key, and a blind value, from the functional value," although Hoffstein et al. do suggest the usage of polynomials in a public key encryption/decryption scheme, as recited below;
- "a public-key obtaining subunit operable to obtain a public key," although Hoffstein et al. do suggest published public key(s), as recited below;

- "a public-key encryption subunit operable to perform a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information," although Hoffstein et al. do suggest public key encryption/decryption scheme using polynomials, as recited below;
- "the public-key encryption algorithm conforms to an NTRU cryptosystem," although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;
- "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key," although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;
- "the public-key encryption subunit generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial," although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];

- "The public key information can be published; that is, made available to any member of the public or to any desired group…" [page 22 lines 12-23];
- "The block 220 represents the routine that can be used by the message sender to encode the plaintext message using the public key of the intended message recipient" [page 22 lines 24-27 & page 23 lines 1-4];
- "1.2 Key Creation. To create an NTRU key" [page 31];
- "Dan randomly chooses…The polynomial f must satisfy the additional requirement… Dan next computes the quantities… Dan's public key is the list of polynomials… Dan's private key is the single polynomial f…" [page 31];
- "1.2 Key Creation…1.3 Encoding…" [page 31];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the shared-key generating unit performs a one-way function on the seed value to generate a functional value, and generates the verification value, the shared key, and a blind value, from the functional value" and "a public-key obtaining subunit operable to obtain a public key" and "a public-key encryption subunit operable to perform a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information" and "the public-key encryption algorithm conforms to an NTRU cryptosystem" and "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key" and "the public-key encryption subunit generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem,

using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial," in the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 11 & 12:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key generation apparatus that notifies a shared-key recovery apparatus about a shared key in secrecy, as in Claim 3 above, but their combination do not disclose,

- "a public-key obtaining subunit operable to obtain a public key," although Hoffstein et al. do suggest published public key(s), as recited below;
- "a public-key encryption subunit operable to perform a public-key encryption algorithm on the verification value, using the public key, to generate the first encryption information," although Hoffstein et al. do suggest public/private key encryption with polynomials, as recited below;
- "the public-key encryption algorithm conforms to an NTRU cryptosystem," although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;
- "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key" although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;

- "the public-key encryption subunit generates a verification-value polynomial from the verification value, generates a blind value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial," although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;

however, Hoffstein et al. do disclose,

- "The public key information can be published; that is, made available to any member of the public or to any desired group…" [page 22 lines 12-23];
- "The block 220 represents the routine that can be used by the message sender to encode the plaintext message using the public key of the intended message recipient" [page 22 lines 24-27 & page 23 lines 1-4];
- "1.2 Key Creation. To create an NTRU key" [page 31];
- "Dan randomly chooses…The polynomial f must satisfy the additional requirement… Dan next computes the quantities… Dan's public key is the list of polynomials… Dan's private key is the single polynomial f…" [page 31];
- "1.2 Key Creation…1.3 Encoding…" [page 31];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a public-key obtaining subunit operable to obtain a public key" and "a public-key obtaining subunit operable to obtain a public key" and "a public-key

encryption subunit operable to perform a public-key encryption algorithm on the verification value, using the public key, to generate the first encryption information" and "the public-key encryption algorithm conforms to an NTRU cryptosystem" and "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key" and "the public-key encryption subunit generates a verification-value polynomial from the verification value, generates a blind value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial," in the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 13-19:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key generation apparatus that notifies a shared-key recovery apparatus about a shared key in secrecy, as in Claim 3 above, but their combination do not disclose,

- "the second encryption unit performs a one-way function on the verification value to generate a functional value, and performs an encryption algorithm, on the seed value, using the functional value, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public key encryption scheme, as recited below;

- "the second encryption unit performs bitwise exclusive-or as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second encryption unit performs a symmetric key encryption algorithm as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second encryption unit performs addition as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second encryption unit performs multiplication as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second encryption unit performs, on the verification value, a hash function as the one-way function, to generate the functional value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;

- "the second encryption unit performs an encryption algorithm on the seed value using the verification value, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula..." [pages 16-17];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the second encryption unit performs a one-way function on the verification value to generate a functional value, and performs an encryption algorithm, on the seed value, using the functional value, to generate the second encryption information" and "the second encryption unit performs bitwise exclusive-or as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information" and "the second encryption unit performs a symmetric key encryption algorithm as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information" and "the second encryption unit performs addition as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information" and "the second encryption unit performs multiplication as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information" and "the second encryption unit performs, on the verification value, a hash function as the one-way function, to generate the functional value" and "the second encryption unit performs an encryption algorithm on the seed value using the verification value, to generate the second encryption information," in

the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 20-22:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key generation apparatus that notifies a shared-key recovery apparatus about a shared key in secrecy, as in Claim 3 above, but their combination do not disclose,

- "the second encryption unit encrypts the seed value using the verification value and the first encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second encryption unit performs a one-way function on the verification value and the first encryption information, to generate the functional value, and performs an encryption algorithm on the seed value using the functional value, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second encryption unit performs bitwise exclusive-or as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [pages 16-17];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the second encryption unit encrypts the seed value using the verification value and the first encryption information" and "the second encryption unit performs a one-way function on the verification value and the first encryption information, to generate the functional value, and performs an encryption algorithm on the seed value using the functional value, to generate the second encryption information" and "the second encryption unit performs bitwise exclusive-or as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information," in the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claim 23:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key generation apparatus that notifies a shared-key recovery apparatus about a shared key in secrecy, as in Claim 3 above, but their combination do not disclose,

- "an obtaining unit operable to obtain a content," although Hoffstein et al. do suggest reception of information, as recited below;
- "an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content," although Hoffstein et al. do suggest public key encryption, as recited below;
- "the transmitting unit further transmits the encrypted content," although Hoffstein et al. do suggest communicating encrypted data, as recited below;

however, Hoffstein et al. do disclose,

- [Fig 4 Box# 420 illustrates receiving data/information];
- "The encoding technique of an embodiment of the public key cryptosystem hereof uses a mixing system based on polynomial algebra and reduction modulo two numbers, p and q, while the decoding technique uses an unmixing system whose validity depends on the elementary probability theory" [page 9];
- "Communication is via transceiver…" [page 8 lines 22-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "an obtaining unit operable to obtain a content" and "an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content" and "the transmitting unit further transmits the encrypted content," in the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 25 & 26:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a verification value and a shared key from the seed value, encrypting the verification value to generate first encryption information, encrypting the seed value based on the verification value to generate second

encryption information, and transmitting the first encryption information and the second encryption information, the shared-key recovery apparatus, as in Claim 24 above, but their combination do not disclose,

- "the shared-key generation apparatus obtains a public key, and performs a public-key encryption algorithm on the verification value, using the public key, to generate the first encryption information," although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;
- "a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key," although Hoffstein et al. do suggest published public key(s), as recited below;
- "a public-key decryption subunit operable to perform a public-key decryption algorithm on the first encryption information, to generate the first decryption verification value, the public-key decryption algorithm corresponding to the public-key encryption algorithm," although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;
- "the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem," although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;
- "the shared-key generation apparatus obtains, as the public key, a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, generates a verification-value polynomial from the verification value, generates a blind value, generates a blind-value polynomial from the blind value, and encrypts the verification-

value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial," although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;

- "the receiving unit receives the first encryption information as a polynomial," although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;
- "the secret-key obtaining subunit obtains, as the secret key, a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem," although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;
- "the public-key decryption subunit decrypts the first encryption information as a polynomial, according to a decryption algorithm corresponding to the NTRU cryptosystem's encryption algorithm, using the secret-key polynomial as a key, to generate a decryption verification-value polynomial, and generates the first decryption verification value from the decryption verification-value polynomial," although Hoffstein et al. do suggest public/private key encryption with polynomials in an NTRU key system, as recited below;

however, Hoffstein et al. do disclose,

- "1.2 Key Creation. To create an NTRU key" [page 31];

- "Dan randomly chooses…The polynomial f must satisfy the additional requirement… Dan next computes the quantities… Dan's public key is the list of polynomials… Dan's private key is the single polynomial f…" [page 31];
- "1.2 Key Creation…1.3 Encoding…" [page 31];
- "The public key information can be published; that is, made available to any member of the public or to any desired group…" [page 22 lines 12-23];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the shared-key generation apparatus obtains a public key, and performs a public-key encryption algorithm on the verification value, using the public key, to generate the first encryption information" and "a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key" and "a public-key decryption subunit operable to perform a public-key decryption algorithm on the first encryption information, to generate the first decryption verification value, the public-key decryption algorithm corresponding to the public-key encryption algorithm" and "the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem" and "the shared-key generation apparatus obtains, as the public key, a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, generates a verification-value polynomial from the verification value, generates a blind value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial" and "the receiving unit receives the first encryption information as

a polynomial" and "the secret-key obtaining subunit obtains, as the secret key, a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem" and "the public-key decryption subunit decrypts the first encryption information as a polynomial, according to a decryption algorithm corresponding to the NTRU cryptosystem's encryption algorithm, using the secret-key polynomial as a key, to generate a decryption verification-value polynomial, and generates the first decryption verification value from the decryption verification-value polynomial," in the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 27-32:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a verification value and a shared key from the seed value, encrypting the verification value to generate first encryption information, encrypting the seed value based on the verification value to generate second encryption information, and transmitting the first encryption information and the second encryption information, the shared-key recovery apparatus, as in Claim 24 above, but their combination do not disclose,

- "the shared-key generation apparatus performs a one-way function on the verification value, to generate a functional value, and performs an encryption algorithm on the seed

value using the functional value, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;

- "the second decryption unit performs the one-way function on the first decryption verification value, to generate a decryption functional value, and performs, on the second encryption information, a decryption algorithm corresponding to the encryption algorithm, using the decryption functional value, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the shared-key generation apparatus performs, on the functional value and the seed value, bitwise exclusive-or as the encryption algorithm, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second decryption unit performs, on the decryption functional value and the second encryption information, bitwise exclusive-or as the decryption algorithm, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the shared-key generation apparatus performs, on the functional value and the seed value, a symmetric key encryption algorithm as the encryption algorithm, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;

- "the second decryption unit performs, on the decryption functional value and the second encryption information, a symmetric key decryption algorithm as the decryption algorithm, to generate the decryption seed value, the symmetric key decryption algorithm corresponding to the symmetric key encryption algorithm," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the shared-key generation apparatus performs, on the functional value and the seed value, addition as the encryption algorithm, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second decryption unit performs, on the decryption functional value and the second encryption information, subtraction as the decryption algorithm, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the shared-key generation apparatus performs, on the functional value and the seed value, multiplication as the encryption algorithm, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second decryption unit performs, on the decryption functional value and the second encryption information, division as the decryption algorithm, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;

- "the shared-key generation apparatus performs, on the verification value, a hash function as the one-way function, to generate the functional value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second decryption unit performs, on the first decryption verification value, the hash function as the one-way function, to generate the decryption functional value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula..." [page 16-17];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the shared-key generation apparatus performs a one-way function on the verification value, to generate a functional value, and performs an encryption algorithm on the seed value using the functional value, to generate the second encryption information" and "the second decryption unit performs the one-way function on the first decryption verification value, to generate a decryption functional value, and performs, on the second encryption information, a decryption algorithm corresponding to the encryption algorithm, using the decryption functional value, to generate the decryption seed value" and "the shared-key generation apparatus performs, on the functional value and the seed value, bitwise exclusive-or as the encryption algorithm, to generate the second encryption information" and "the second decryption unit performs, on the decryption functional value and the second

encryption information, bitwise exclusive-or as the decryption algorithm, to generate the decryption seed value" and "the shared-key generation apparatus performs, on the functional value and the seed value, a symmetric key encryption algorithm as the encryption algorithm, to generate the second encryption information" and "the second decryption unit performs, on the decryption functional value and the second encryption information, a symmetric key decryption algorithm as the decryption algorithm, to generate the decryption seed value, the symmetric key decryption algorithm corresponding to the symmetric key encryption algorithm" and "the shared-key generation apparatus performs, on the functional value and the seed value, addition as the encryption algorithm, to generate the second encryption information" and "the second decryption unit performs, on the decryption functional value and the second encryption information, subtraction as the decryption algorithm, to generate the decryption seed value" and "the shared-key generation apparatus performs, on the functional value and the seed value, multiplication as the encryption algorithm, to generate the second encryption information" and "the second decryption unit performs, on the decryption functional value and the second encryption information, division as the decryption algorithm, to generate the decryption seed value" and "the shared-key generation apparatus performs, on the verification value, a hash function as the one-way function, to generate the functional value" and "the second decryption unit performs, on the first decryption verification value, the hash function as the one-way function, to generate the decryption functional value," in the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 33-36:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a verification value and a shared key from the seed value, encrypting the verification value to generate first encryption information, encrypting the seed value based on the verification value to generate second encryption information, and transmitting the first encryption information and the second encryption information, the shared-key recovery apparatus, as in Claim 24 above, but their combination do not disclose,

- "the shared-key generation apparatus performs an encryption algorithm on the seed value using the verification value, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second decryption unit performs a decryption algorithm corresponding to the encryption algorithm, on the second encryption information using the first decryption verification value, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the shared-key generation apparatus encrypts the seed value using the verification value and the first encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;

- "the second decryption unit decrypts the second encryption information, using the first decryption verification value and the first encryption information, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the shared-key generation apparatus performs, on the functional value and the seed value, multiplication as the encryption algorithm, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second decryption unit performs the one-way function on the first decryption verification value and the first encryption information, to generate a decryption functional value, and performs a decryption algorithm corresponding to the encryption algorithm, on the second encryption information, using the decryption functional value, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the shared-key generation apparatus performs bitwise exclusive-or as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption scheme, as recited below;
- "the second decryption unit performs bitwise exclusive-or as the decryption algorithm, on the decryption functional value and the second encryption information, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the shared-key generation apparatus performs an encryption algorithm on the seed value using the verification value, to generate the second encryption information" and "the second decryption unit performs a decryption algorithm corresponding to the encryption algorithm, on the second encryption information using the first decryption verification value, to generate the decryption seed value" and "the shared-key generation apparatus encrypts the seed value using the verification value and the first encryption information" and "the second decryption unit decrypts the second encryption information, using the first decryption verification value and the first encryption information, to generate the decryption seed value" and "the shared-key generation apparatus performs, on the functional value and the seed value, multiplication as the encryption algorithm, to generate the second encryption information" and "the second decryption unit performs the one-way function on the first decryption verification value and the first encryption information, to generate a decryption functional value, and performs a decryption algorithm corresponding to the encryption algorithm, on the second encryption information, using the decryption functional value, to generate the decryption seed value" and "the shared-key generation apparatus performs bitwise exclusive-or as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information" and "the second decryption unit performs bitwise exclusive-or as the decryption algorithm, on the decryption functional value and the second encryption

information, to generate the decryption seed value," in the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 37-39:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a verification value and a shared key from the seed value, encrypting the verification value to generate first encryption information, encrypting the seed value based on the verification value to generate second encryption information, and transmitting the first encryption information and the second encryption information, the shared-key recovery apparatus, as in Claim 24 above, but their combination do not disclose,

- "the shared-key generation apparatus performs a one-way function on the seed value, to generate a functional value, and generates the verification value and the shared key from the functional value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the shared-key generating unit performs the one-way function on the decryption seed value, to generate a decryption functional value, and generates the second decryption verification value and the decryption shared key from the decryption functional value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;

- "the shared-key generation apparatus performs, on the seed value, a hash function as the one-way function, to generate the functional value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the shared-key generating unit performs, on the decryption seed value, the hash function as the one-way function, to generate the decryption functional value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the shared-key generation apparatus generates the verification value by setting a part of the functional value as the verification value, and generates the shared key by setting another part of the functional value as the shared key," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the shared-key generating unit generates the second decryption verification value by setting a part of the decryption functional value as the second decryption verification value, and generates the decryption shared key by setting another part of the decryption functional value as the decryption shared key," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the shared-key generation apparatus performs a one-way function on the seed value, to generate a functional value, and generates the verification value and the shared key from the functional value" and "the shared-key generating unit performs the one-way function on the decryption seed value, to generate a decryption functional value, and generates the second decryption verification value and the decryption shared key from the decryption functional value" and "the shared-key generation apparatus performs, on the seed value, a hash function as the one-way function, to generate the functional value" and "the shared-key generating unit performs, on the decryption seed value, the hash function as the one-way function, to generate the decryption functional value" and "the shared-key generation apparatus generates the verification value by setting a part of the functional value as the verification value, and generates the shared key by setting another part of the functional value as the shared key" and "the shared-key generating unit generates the second decryption verification value by setting a part of the decryption functional value as the second decryption verification value, and generates the decryption shared key by setting another part of the decryption functional value as the decryption shared key," in the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 40-43:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a verification value and a shared key from the seed value, encrypting the verification value to generate first encryption information, encrypting the seed value based on the verification value to generate second encryption information, and transmitting the first encryption information and the second encryption information, the shared-key recovery apparatus, as in Claim 24 above, but their combination do not disclose,

- "the shared-key generation apparatus performs a one-way function on the seed value, to generate a functional value, generates the verification value, the shared key, and a blind value, from the functional value, obtains a public key, and performs a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the shared-key generating unit performs the one-way function on the decryption seed value, to generate a decryption functional value, and generates, from the decryption functional value, the second decryption verification value, the decryption shared key, and the decryption blind value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;

- "the shared-key generation apparatus obtains a public key, performs a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the judging unit, instead of performing the judging based on the first decryption verification value and the second decryption verification value, includes: a public-key obtaining subunit operable to obtain the public key," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the judging unit, instead of performing the judging based on the first decryption verification value and the second decryption verification value, includes: a re-encryption subunit operable to perform the public-key encryption algorithm on one of the first decryption verification value and the second decryption verification value, using the public key and the decryption blind value, to generate re-encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the judging unit, instead of performing the judging based on the first decryption verification value and the second decryption verification value, includes: a judging subunit operable to judge, based on the first encryption information and the re-encryption information, whether the decryption shared key should be outputted or not," although

Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;

- "the judging subunit compares the first encryption information and the re-encryption information, thereby judging that the decryption shared key should be outputted if the first encryption information is identical to the re-encryption information," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the public-key encryption algorithm conforms to an NTRU cryptosystem," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme in an NTRU cryptosystem, as recited below;
- "the shared-key generation apparatus obtains, as the public key, a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme in an NTRU cryptosystem, as recited below;
- "the public-key obtaining subunit obtains the public-key polynomial," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;

- "the re-encryption subunit generates a decryption verification-value polynomial from the second decryption verification value, generates a decryption blind-value polynomial from the decryption blind value, and encrypts the decryption verification-value polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the decryption blind-value polynomial to randomize the decryption verification value polynomial, to generate the re-encryption information as a polynomial," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];
- [Fig 6 Box# 640 illustrates verification];
- "Finally Dan computes…to recover the original message m" [page 20];
- "1.2 Key Creation. To create an NTRU key" [page 31];
- "Dan randomly chooses…The polynomial f must satisfy the additional requirement… Dan next computes the quantities… Dan's public key is the list of polynomials… Dan's private key is the single polynomial f…" [page 31];
- "1.2 Key Creation…1.3 Encoding…" [page 31];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the shared-key generation apparatus performs a one-way function on the seed value, to generate a functional value, generates the verification value, the shared key, and a blind value, from the functional value, obtains a public key, and performs a

public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information" and "the shared-key generating unit performs the one-way function on the decryption seed value, to generate a decryption functional value, and generates, from the decryption functional value, the second decryption verification value, the decryption shared key, and the decryption blind value" and "the shared-key generation apparatus obtains a public key, performs a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information" and "the judging unit, instead of performing the judging based on the first decryption verification value and the second decryption verification value, includes: a public-key obtaining subunit operable to obtain the public key" and "the judging unit, instead of performing the judging based on the first decryption verification value and the second decryption verification value, includes: a re-encryption subunit operable to perform the public-key encryption algorithm on one of the first decryption verification value and the second decryption verification value, using the public key and the decryption blind value, to generate re-encryption information" and "the judging unit, instead of performing the judging based on the first decryption verification value and the second decryption verification value, includes: a judging subunit operable to judge, based on the first encryption information and the re-encryption information, whether the decryption shared key should be outputted or not" and "the judging subunit compares the first encryption information and the re-encryption information, thereby judging that the decryption shared key should be outputted if the first encryption information is identical to the re-encryption information" and "the public-key encryption algorithm conforms to an NTRU cryptosystem" and "the shared-key generation apparatus obtains, as the public key, a public-key polynomial generated according to

a key-generation algorithm of the NTRU cryptosystem, generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial" and "the public-key obtaining subunit obtains the public-key polynomial" and "the re-encryption subunit generates a decryption verification-value polynomial from the second decryption verification value, generates a decryption blind-value polynomial from the decryption blind value, and encrypts the decryption verification-value polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the decryption blind-value polynomial to randomize the decryption verification value polynomial, to generate the re-encryption information as a polynomial," in the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 44 & 45:

Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) disclose a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a verification value and a shared key from the seed value, encrypting the verification value to generate first encryption information, encrypting the seed value based on the verification value to generate second

encryption information, and transmitting the first encryption information and the second encryption information, the shared-key recovery apparatus, as in Claim 3 above, but their combination do not disclose,

- "the judging unit compares the first decryption verification value and the second decryption verification value, thereby judging that the decryption shared key should be outputted if the first decryption verification value is identical to the second decryption verification value," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the shared-key generation apparatus further obtains a content, encrypts the content using the shared key to generate an encrypted content and transmits the encrypted content," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the receiving unit further receives the encrypted content," although Hoffstein et al. do suggest receiving encrypted data/information, as recited below;
- "the shared-key recovery apparatus further comprises: a decryption unit operable to decrypt the received encrypted content using the decryption shared key, to generate a decrypted content," although Hoffstein et al. do suggest the usage of polynomials in a public/private key encryption/decryption scheme, as recited below;
- "the shared-key recovery apparatus further comprises: an outputting unit operable to output the decrypted content," although Hoffstein et al. do suggest decrypting encrypted data/information to obtain the decrypted data/information, as recited below;

however, Hoffstein et al. do disclose,

- "Finally Dan computes…to recover the original message m" [page 20];
- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];
- [Fig 5 Box# 530 illustrates receiving encrypted data/information];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the judging unit compares the first decryption verification value and the second decryption verification value, thereby judging that the decryption shared key should be outputted if the first decryption verification value is identical to the second decryption verification value" and "the shared-key generation apparatus further obtains a content, encrypts the content using the shared key to generate an encrypted content and transmits the encrypted content" and "the receiving unit further receives the encrypted content" and "the shared-key recovery apparatus further comprises: a decryption unit operable to decrypt the received encrypted content using the decryption shared key, to generate a decrypted content" and "the shared-key recovery apparatus further comprises: an outputting unit operable to output the decrypted content," in the invention as disclosed by Gennaro et al. (US-5937066-A) and Gennaro et al. (US-5907618-A) for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Response to Arguments

5. Applicant's arguments with respect to claims 1-47, 49, & 50 have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicant's amendments.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

a. Hoffstein et al. (US-20030120929-A1) – NTRU cryptosystem

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
03/20/2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136